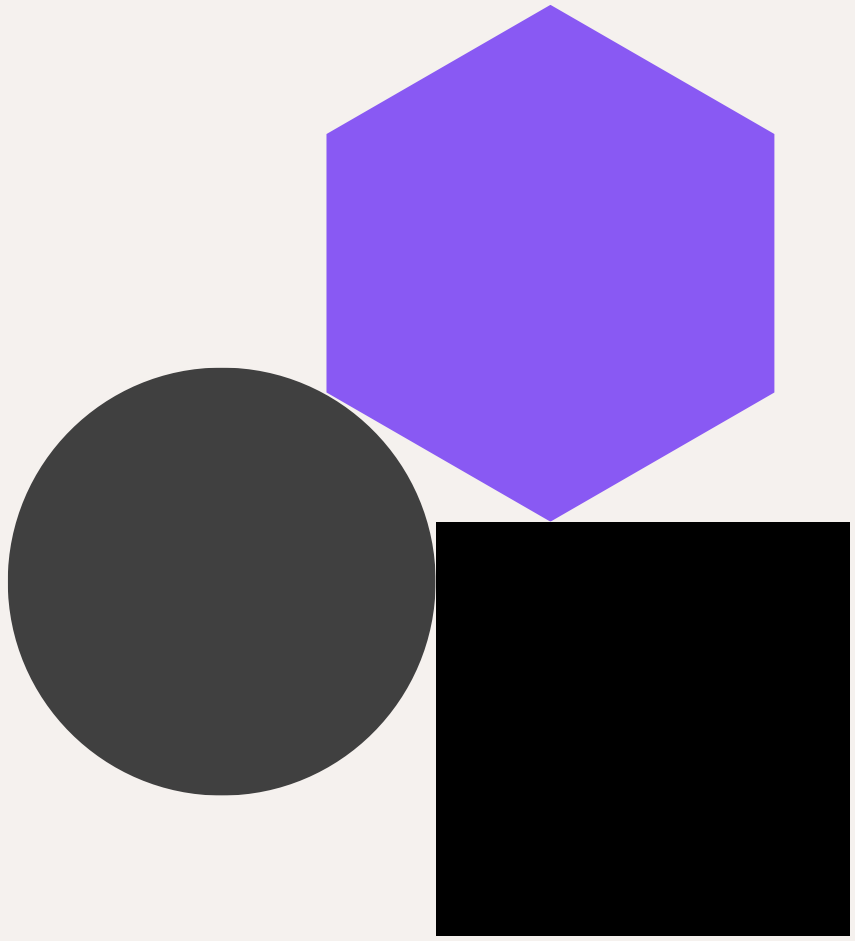
CHERI Linux

Codasip



Status update

Carl Shaw

CHERI Blossoms conference, April 2025

→ Agenda

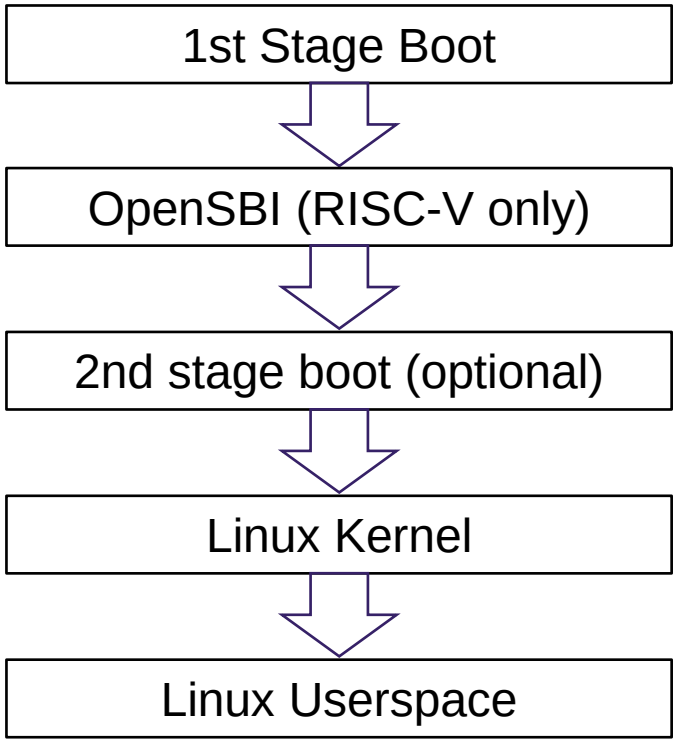
Codasip

- Where we are now
- What's next?

→ Where we are now

→ CHERI Linux kernel

- **Pure capability software stack**
- Currently on kernel v6.10
- Started with Morello hybrid kernel code
- Initial goals:
  - Functionality
  - Security : spatial memory safety
- Diffstat:
  - 4133 files changed
  - 115253 insertions(+)
  - 17312 deletions(-)



Purecap embedded Linux boot flow

→ Kernel functionality

Codasip

- Now building kernel (mostly) allyesconfig
  - Compiling but not necessarily tested
  - Still have a number of drivers disabled
  - Major features fully or partially disabled: CONFIG_RELOCATABLE, KEXEC, KVM and virtualization, eBPF, JUMP_LABEL, modules, NTFS3, ACPI, EFI/UEFI, CONFIG_INFINIBAND
- Testing kernel using LTP
  - 2/3 of standard tests passing
- Making good progress on testing driver subsystems with real hardware
  - PCIe, USB, network (wired and wireless), audio, graphics

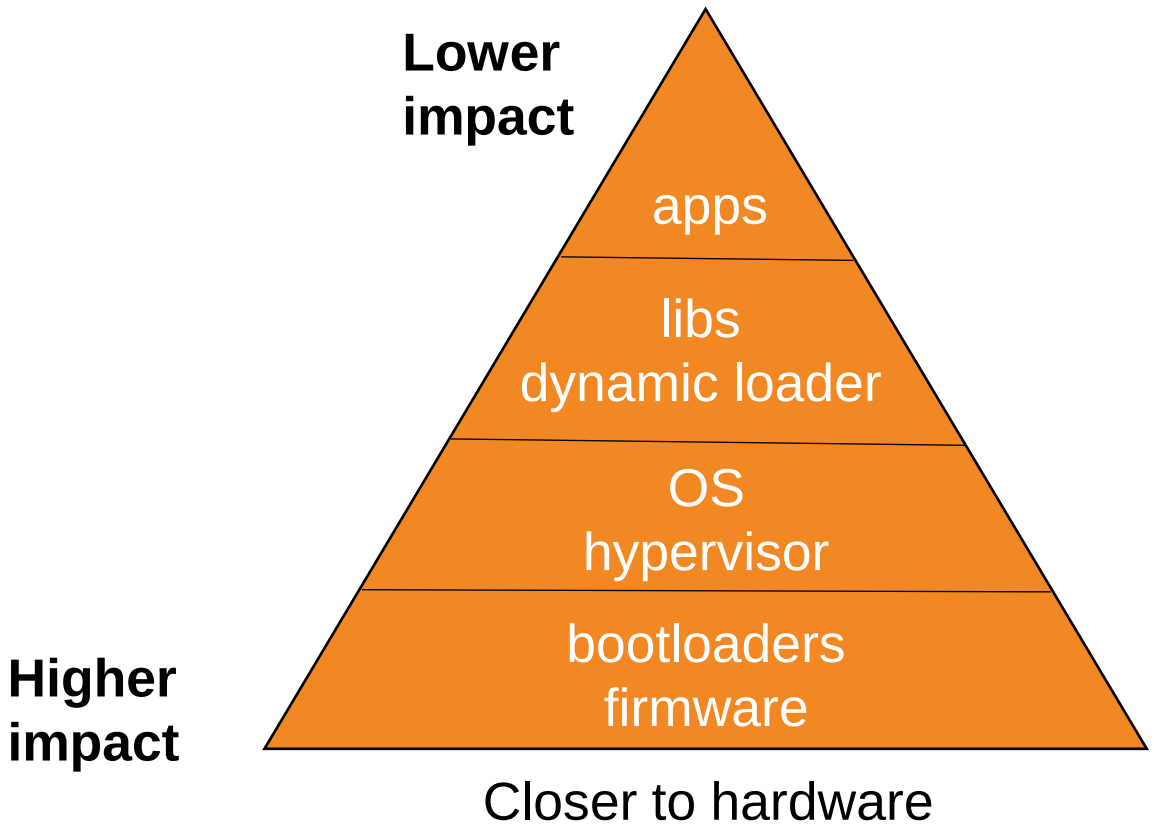
→ Kernel security

Codasip

- Trying to restrict bounds to minimum possible
  - Some have to be generated as we have to convert an integer address to a capability
    - Example: virt_to_phys()

→ Linux userspace

- Yocto based Linux distribution
- Rapidly increasing packages working
- Reused patches from CHERI BSD
- Modern packages require little (if any) modification
  - C++ better than C



→ What's next?

→ Next steps

Codasip

- Create base CHERI Alliance CHERI Linux kernel
  - Rebase kernel against v6.14?
  - Remove support for older CHERI-RISC-V draft versions
  - Ensure clean history
  - Make kernel repo public!
- Push Yocto build system to new repo
- Move forward!!
- Get involved by joining the CHERI Alliance Linux Working Group

→ Next steps from Codasip (CHERI-RISC-V)

Codasip

- Upcoming kernel work:
  - Hybrid kernel ABI
  - Loadable module support
  - Sub-object bounds
  - eBPF
  - More device support
- User space:
  - Wireless networking support
  - Start on full Linux distribution
- Performance optimisation
  - Profiling support
  - String functions
  - Memory allocators
  - Compiler optimisations
- FPGA platform!
  - Codasip X730 application core

Codasip

→

Thank you!

For more information:

https://cheri-alliance.org/

https://cheri-linux.org/

X730 CHERI application core:

https://codasip.com/solutions/riscv-processor-safety-security/cheri/x730-risc-v-application-processor/

carl.shaw@codasip.com